

COMPLIANCE WEEK

THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

Security Control Threats in Tight IT Budgets

By Todd Neff — January 27, 2009

For all the improvements companies have made to their IT security and control systems in the last five years, one menace still looms large these days: that layoffs will wreck the compliance system you've carefully crafted.

The most significant threats to a company have always lurked within its own walls. Now, as job security diminishes with each earnings report and layoff announcement, employees are increasingly looking out for number one, says Adam Bosnian, head of sales and strategy for information security software firm Cyber-Ark. In a recent survey of 247 Wall Street workers, Cyber-Ark found that 58 percent would pre-emptively download corporate data if they felt their jobs were at risk; 62 percent saying doing so would be easy.

Then there's the problem of outside threats, which remain as constant as ever—even while companies are laying off IT staff or cutting IT security spending that might block those invaders. Data breaches cost an average of nearly \$200 per record, according to a November 2007 Ponemon Institute study that considered 35 businesses that suffered breaches. Sixty-five percent of the cost was in lost business, the study found.

David Cowings, senior manager for Symantec Security Response, says his company has seen an uptick in Web advertising for stolen data, with premiums on birthdates, social security numbers supporting identity theft and, of course, credit card numbers.

So let's recap: Not only must a compliance officer worry about unhappy or fearful workers; you must worry about newly opened holes in the organizational chart that hackers might exploit as well.

There are ways of stopping—or at least deterring—either kind of threat. Software from firms like Cyber-Ark encrypt data and track access so that would-be scofflaws either are stopped or leave a clearly visible audit trail. Other data loss prevention systems focus on “endpoint security;” that can involve everything from recognizing credit card numbers or dates of birth in outgoing e-mails to blocking the copying of certain data to memory sticks.

If layoffs do happen, strong termination and de-provisioning processes ensuring immediate cutoff of IT access are vital, says Tom DeSot, chief compliance officer of San Antonio, Texas-based Digital Defense.

Bosnian says companies should particularly focus on “power users” such as database and system administrators, whose access privileges and lack of traceability (companies often have a single administrator password shared among users, he says) present risk of catastrophic loss. Yes, he says, sweeping regulations such as the HIPAA privacy law may limit data access for 1,000 doctors and 2,000 nurses in a hospital, “but it can be a small population of 20 admins that pose the largest threat,” he said.

To fend off outside threats, Cowings advises companies to consider consolidating vendors to manage security solutions and, particularly for small and medium-sized businesses, to consider outsourcing security altogether.

Jason Lidow, founder of DigiTrust Group, which specializes in managed security services for small business, says such companies are particularly vulnerable; they may have less data at stake, but they have softer underbellies. (And even if thieves are caught, they usually face smaller penalties, he adds.)

The Layoff Factor

If merely the threat of downsizing can heighten insider IT security risks, the act of downsizing certainly exacerbates it. In most cases, layoffs are reactionary: The CEO tells the CIO simply to cut costs, and the CIO gives his department heads a budget number to hit. Cutting jobs is the easiest way to do that quickly.

Jeff Camiel, technology risk manager for Jefferson Wells, says IT security is often a victim: Despite preventing enormous losses, it is always a budget hog. That can hurt in several ways. The fewer employees who remain must do more work, which leads to expanded access privileges and heightened insider risk. At the same time, diligent employees might be too busy to execute all their duties with proper care, or to notice errant employees committing some impropriety.

In such an environment, Camiel suggests doing (or redoing) comprehensive IT risk assessments to understand how risks have shifted and what the new costs of various IT governance methods really are.

“You may find redundant layers of security, and if they can be re-architected, you may be in better shape at lower cost,” Camiel says.

But IT security spending may at least be somewhat insulated from budget cuts, according to a recent Forrester Research report, *The State of Enterprise IT Security: 2008 to 2009*. About 2,150 North American and European IT executives surveyed said they expected IT security spending to rise from 11.7 percent of IT budgets in 2008 to 12.6 percent in 2009.

Although the survey data came in just before the September 2008 financial meltdown, Jonathan Penn, Forrester Research’s vice president for security technology strategy, says he still doesn’t expect drastic cutbacks.

“As for what to do during a period of intense budgetary—and, especially, capital expenditure—pressures, we see more of a focus on projects being justified for the operational efficiency gains obtained, and we see more interest in security outsourcing and managed services,” he says.

DeSot says that makes sense, considering the realities of the Graham Leach Bliley Act, HIPAA, PCI security regulations, the Sarbanes-Oxley Act and other regulations.

“What I’ve seen is that the programs in place now tend to be much more robust and much more serious than I’d see even five years ago,” he says. “I think it’s a direct by-product of regulations and the large amount of pressure on organizations to maintain compliance.”

For companies facing cost pressures, Penn suggests using metrics to justify spending, outsourcing security to reduce headcount, and prioritizing projects to delay those without a near-term payoff—which has an added benefit of building political capital for later office battles, he says.

Howard Schmidt, a former White House IT security adviser and now president and CEO of the Information Security Forum, says companies can delay such things as implementing smart card or USB-dongle-based authentication (both expensive undertakings) by adding cheaper systems that track such things as from where users are logging in.

He also suggests negotiating with IT security vendors, who now have to be more competitive. Security is non-negotiable, he says, but the price of tools to help maintain it often is.

“As people tighten their belts, it’s not a matter of either-or,” Schmidt says. “It’s a matter of how we get where we need to be without spending the money we would normally spend.”

WHAT WOULD YOU TAKE?

If you were fired tomorrow what information would you try & take with you?

Answer:	UK	USA	Holland
I wouldn't take any information with me	41%	42%	2%
Customer & Contacts Database	25%	52%	31%
Product Information	11%	30%	15%
Plans and proposals	17%	31%	16%
HR Records	6%	28%	8%
Access and Password Codes	13%	35%	15%
Legal records	6%	23%	4%
Other	2%	8%	9%

Source

Cyber-Ark: The Global Recession and Its Effect on Work Ethics (December 2008).

EASY STEAL?

Is it easy to take sensitive/valuable information out of your company?

Answer:	UK	USA	Holland
Yes	29%	62%	54%
No	71%	38%	46%

Source

Cyber-Ark: The Global Recession and Its Effect on Work Ethics (December 2008).

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.